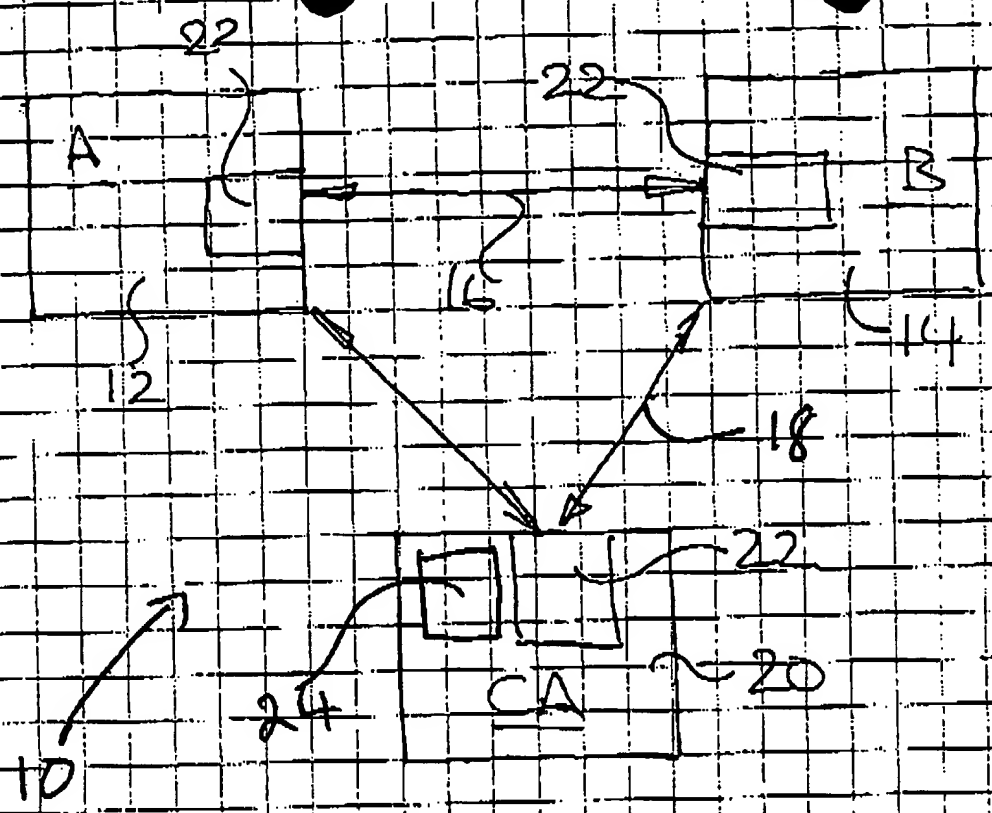

Fig. 1

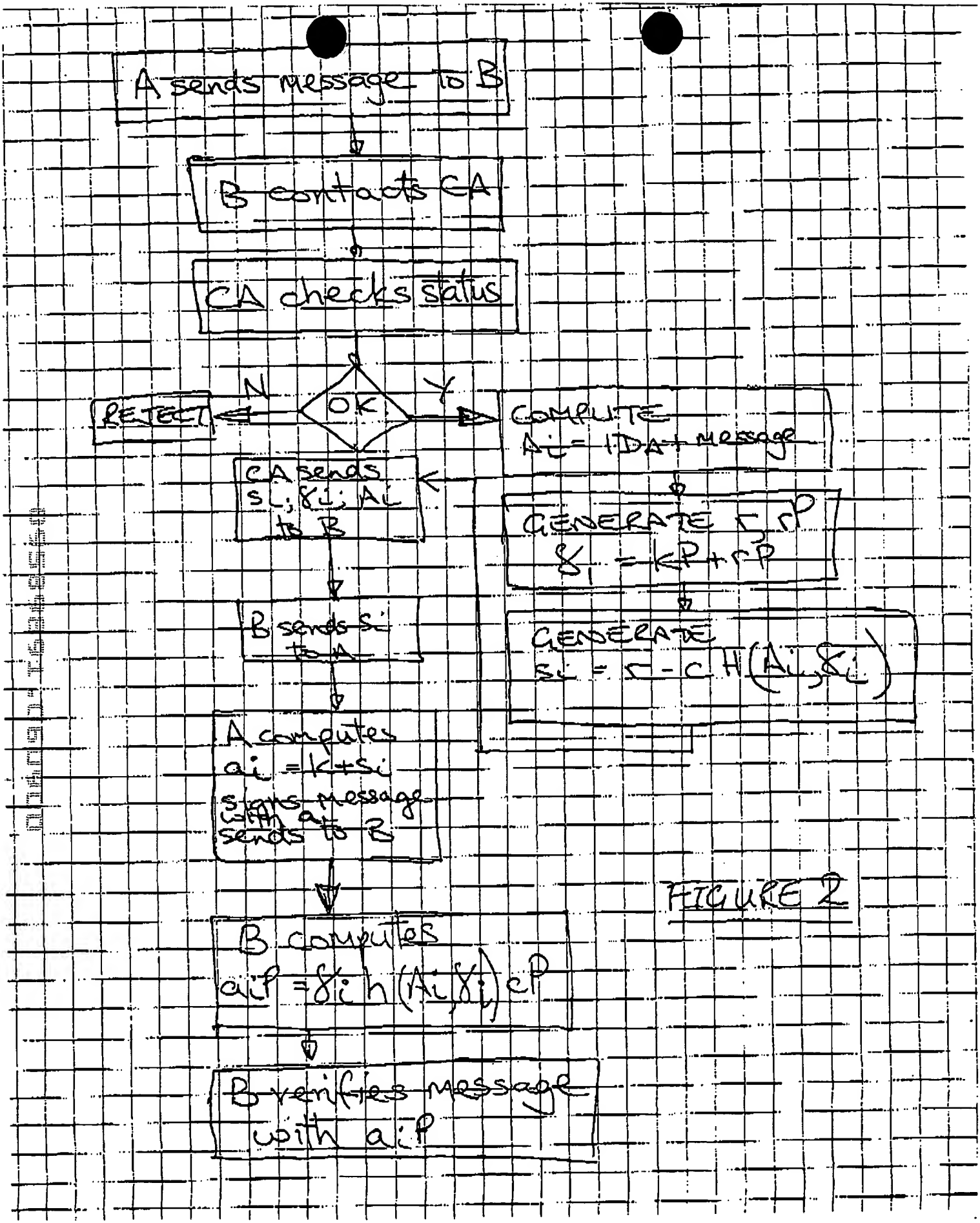
A sends message to B
B contacts CA
CA checks status
OK
N
Y
REJECT
COMPUTE
Ai = IDA + message
GENERATE r, rP
δi = kP + rP
GENERATE
si = r - c H(Ai, δi)
CA sends
si; δi; Ai
to B
B sends si
to A
A computes
ai = k + si
signs message
with ai
sends to B
B computes
aiP = δi h(Ai, δi) cP
B verifies message
with aiP

FIGURE 2

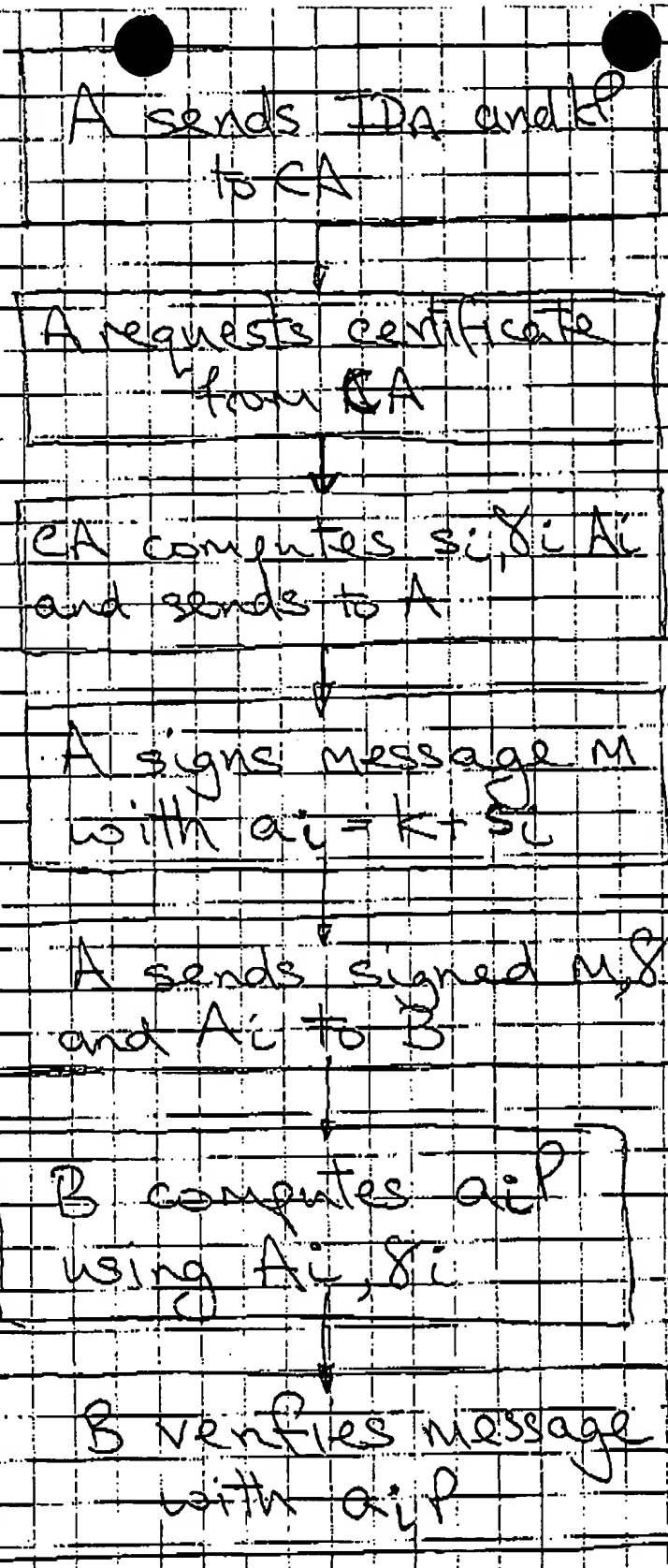
A sends IDA and k^e to CA
A requests certificate from CA
CA computes si, δi Ai and sends to A
A signs message M with ai = k + Si
A sends signed M, δi and Ai to B
B computes ai^p using Ai, δi
B verifies message with ai^p

FIGURE 3

A sends ID_A and k^p to CA

A requests certificate from CA

CA uses ID_A and a permission level to determine A_i

CA generates s_i, δ_i based on A_i and send all 3 to A

A signs message, M, with $a_i = k + s_i$

A sends signed M, δ_i and A_i To B

B computes a_i^p using A_i, δ_i

B verifies message with a_i^p

B grants A access to an application

FIGURE 4

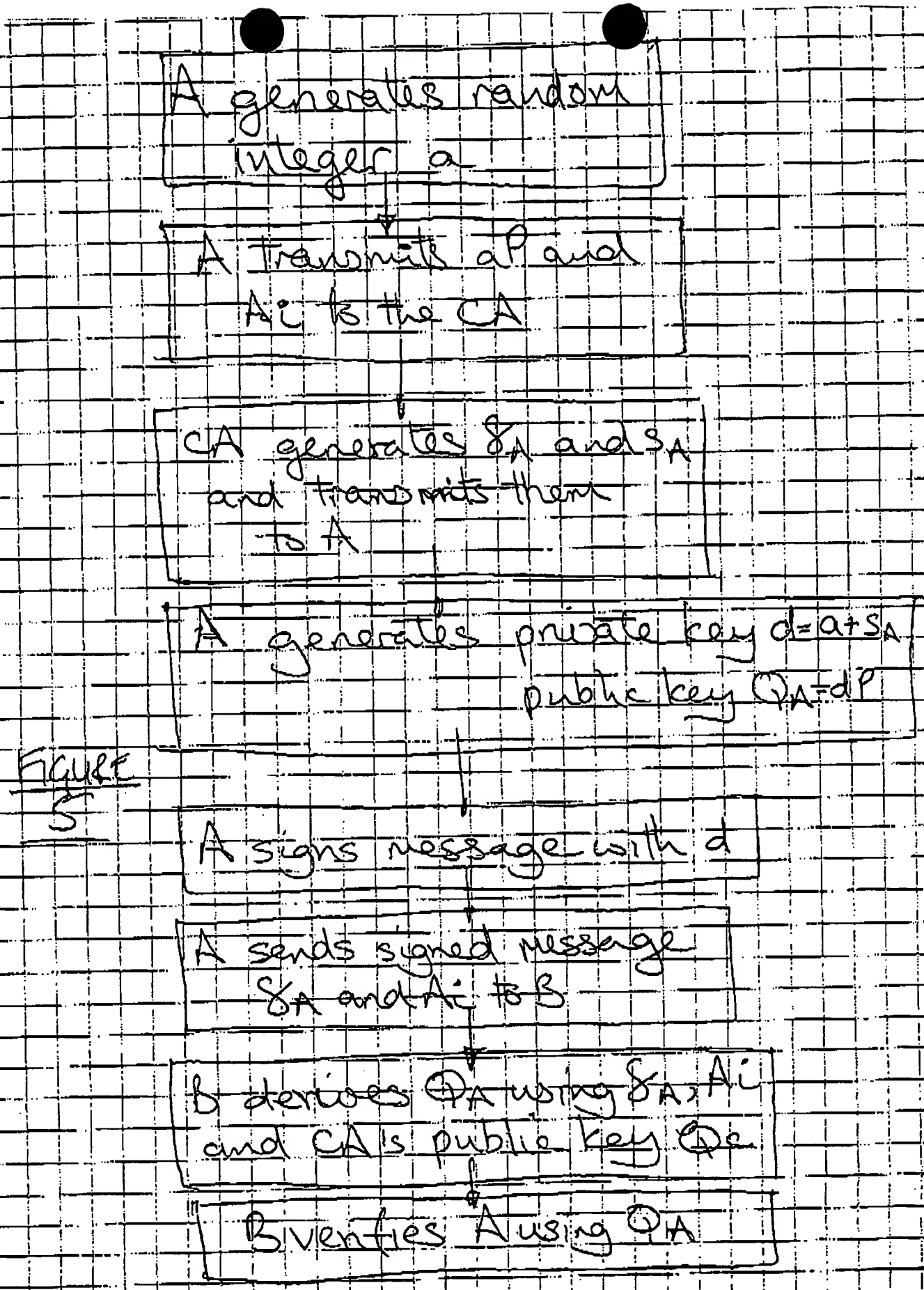
A generates random integer a
A transmits dP and Ai to the CA
CA generates δ_A and s_A and transmits them to A
A generates private key $d = a + s_A$ public key $Q_A = dP$
A signs message with d
A sends signed message δ_A and Ai to B
B derives Q_A using δ_A, Ai and CA's public key Q_{CA}
B verifies A using Q_A

FIGURE 5

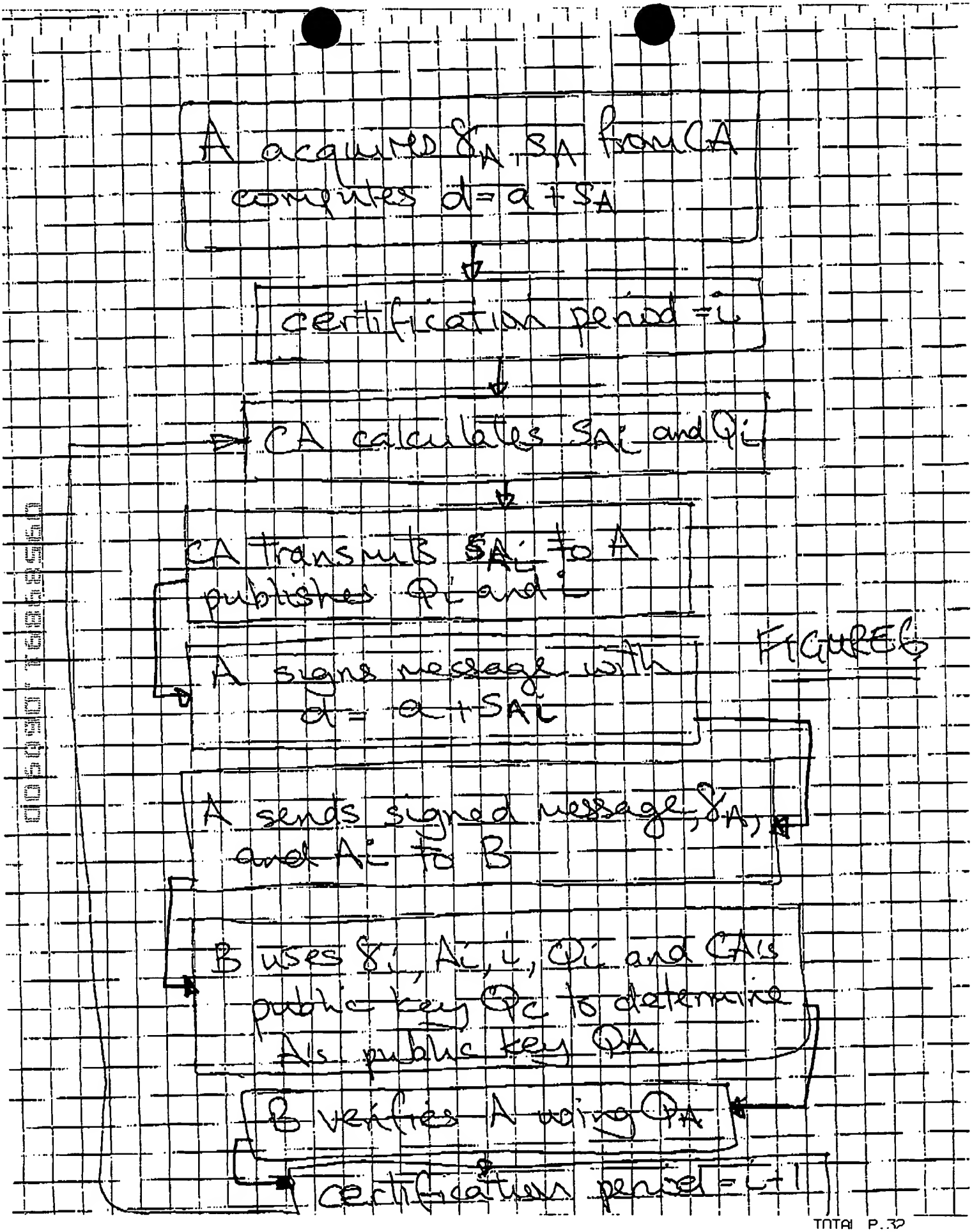
A acquires S_A, S_A from CA
computes $d = a + S_A$
certification period = i
CA calculates S_{A_i} and Q_i
CA transmits S_{A_i} to A
publishes Q_i and i
A signs message with $d = a + S_{A_i}$
A sends signed message, S_A, and A_i to B
B uses S_i, A_i, i, Q_i and CA's public key Q_c to determine A's public key Q_A
B verifies A using Q_A
certificates period = i+1

FIGURE 6